Privacy Officer Information Packet
2019 External Packet Issue 8

Tools for communicating about privacy at the U.S. Department of Veterans Affairs

VA Privacy Service | **Hotline:** 202-273-5070
Email: vaprivacycommunications@va.gov
Web: www.va.gov/privacy

PRIVACY MATTERS VA

How To Protect Your Privacy When You Travel

This article originally appeared in Forbes.

For those living in the Northern Hemisphere, summer travel beckons! Before you take off on your family vacation or business trip, however, here are simple ways to keep safe and protect your privacy while you're on the road or in a foreign land.

1. Keep important documents at your fingertips

We've all been there — when dread takes hold and you realize you've misplaced your wallet or purse. Even worse is when you realize you are now without your passport, credit cards, health insurance card, and driver's license. Make copies and store them in a safe place or, better yet, take pictures of your IDs and credit cards and lock them down with Keepsafe Photo Vault on iOS or Android. You'll rest easier knowing that you've got backups with you in case your belongings are lost or stolen.

2. Set passcodes & encrypt

Don't travel (or go anywhere really) without setting a passcode on your mobile phone and/or laptop and ensuring it's encrypted. (Follow instructions for how to encrypt your devices here.) When you have a strong password and encrypted devices, thieves can't access your materials and accounts. Even if your devices go

missing, your privacy remains protected. You can safeguard your apps with an added level of security with AppLock on Android. Set a PIN or pattern code to lock-down apps so that they can't be broken into. Protect your email, messaging apps, social media, finance and shopping apps from being compromised.

3. Be deliberate about traveling with apps

More people are reporting having their mobile phones searched when traveling internationally and/or entering or re-entering the US. (Digital searches at the border increased by 5 times between 2015 and 2016.) Consider deleting sensitive materials (like work documents) or apps that you don't want accessed. Most apps require an account login so you can always re-install them when you return home. If you use a Password Manager like 1Password to keep track of your passwords, use Travel Mode. Travel Mode allows you to designate which passwords are safe to keep with you while traveling. Others get removed from your password vaults until you login and turn off Travel Mode. This is another great way to protect sensitive work accounts from being accessed or searched (admins can also manage what accounts employees have access to while traveling).

4. Use a VPN and be sure to logout

When you travel, you are more likely to use a free Wi-Fi hotspot to get online. You may use an unsecured public network to access the internet in an airport, hotel or cafe. VPNs, or virtual private networks, are tunnels that encrypt your browsing and internet activity and obscure your IP address, so they stay private. Even if there are eavesdroppers listening in on public networks (yes, that's possible), you can safely go about your business wherever you are. Make sure you use a legitimate VPN service that you pay for and trust to maintain your privacy. If you're accessing your email or other accounts using a hotel Business Center or internet cafe, make sure you log out of any personal accounts so others don't happen upon sensitive information and can't impersonate you or hijack your accounts.

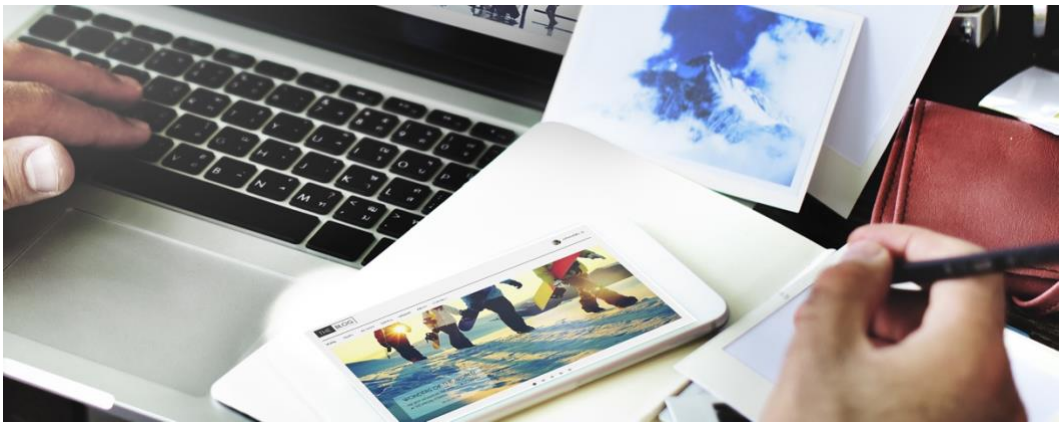
5. Invest in a burner phone and/or laptop

If you really want to protect private materials on your phone or laptop, consider traveling with lower-end, lower cost pre-paid devices. You can still make phone

calls, get help and access the internet, but traveling lighter means lowering the risk of having your privacy compromised if your device is lost, stolen or searched. (And by the way, there are plenty of other reasons for having burner devices beyond just travel!)

Travel safely and protect yourself when vacationing this summer. Just as you keep cash out of sight when you're on the street and lock valuables in your hotel safe, make sure you preserve your digital life when you're away from home. Take precautions so you can enjoy your trip and rest easy. ■

7 Essential Privacy Tips for When You Travel



This article originally appeared in Toms Guide.

Airports, hotel rooms and rental cars pose unseen privacy risks. Here's what to do.

American travelers took 2.25 billion domestic trips and 87.7 million international trips in 2017, according to statistics from the U.S. Travel Association and the U.S. National Travel and Tourism Office. If you were one of those travelers, you likely walked through a body scanner, had your photo taken to confirm your identity, or gave up personal data without even realizing it.

You may have also encountered "smart" hotel rooms in which a tablet controlled the lights, curtains and temperature, and perhaps even saved your preferences for your next stay. When you drove off in your rental car, you may not have realized that the rental company was collecting data on your driving habits and the car's location. And when you logged in to that hotel Wi-Fi network, you had no idea who else might be on the same network.

Of course, none of these practices are illegal. But they all raise the risks that your private personal data may be misused, misappropriated or stolen. Fortunately, there are ways you can try to minimize the data collection.

Quick Travel Privacy Tips

- If you're uncomfortable with facial-recognition systems or body scanners at U.S. airport security checkpoints, you can opt out (travelers can usually request a pat-down instead).
- Use a VPN whenever you're on a Wi-Fi network, including in your hotel room.
- Turn off the Wi-Fi, GPS and Bluetooth functions on your smartphone when you're not using them.
- Travel tech can be both cheap and simple: bring a Chromebook instead of a laptop, and log out of and shut down the machine before crossing international borders.
- Bring a cheap Android phone instead of your regular smartphone.
- Consider setting up "fake" online accounts before you travel, in case border officials want to see them.
- Before you return a rental car, try to delete any navigation history or personal profile you set up in a rented GPS device or in the in-vehicle navigation system.

Dealing with creepy airport screening technology

Since 2016, the U.S. Customs and Border Protection's (CBP) Biometric Air Exit program has put facial-recognition technology in several U.S. airports. When you board an international flight, CBP or a partner airline takes a picture of you and compares it against your passport photo. Delta and JetBlue already participate in this program.

The Transportation Security Administration recently launched a similar pilot program for international flights at Los Angeles International Airport in which departing travelers can opt to have their photos used to verify that their boarding passes and passports match. (LAX has been named “most innovative airport -- large hub” by the American Association of Airport Executives.)

If there is a discrepancy, travelers are not allowed through the security checkpoint — although TSA agents will still be able to manually verify their boarding documents.

CBP aims to use biometrics to confirm the identities of more than 97 percent of passengers in the next few years and to expand this initiative to every point of entry and exit in the United States. Facial recognition isn't 100 percent accurate, however — it more frequently misidentifies ethnic minorities and people wearing certain accessories or makeup, *Quartz* reported.

Jeramie Scott, director of Domestic Surveillance Project of the Electronic Privacy Information Center (EPIC), said facial recognition as a primary means of identification heightens the capacity of the government to conduct surveillance beyond the scope of confirming travelers' identities. Scott worries that this data could be used in ways we haven't consented to — although CBP says images are deleted and purged from its systems within 14 days.

"There need to be protections around the collection and use of certain data," Scott told Tom's Guide. "If you agree to use your face as your boarding pass and confirm your identity that way, there should be rules in place that prevent that use from going beyond that stated purpose."

Scott said that, if you don't like the notion of facial-recognition software, you should be able to opt out of biometric screening to board flights by requesting an alternative review from a CBP official.

The same goes for body scanners, which used to essentially render you naked on a TSA computer screen, but now display a generic body outline. If that still makes you uncomfortable, you have two choices as long as you're at a U.S. security checkpoint.

The first option is to sign up for the TSA's Precheck program. You'll have to pay $85 (good for five years), submit your fingerprints, and agree to a background check.

If you're accepted, then you'll be walking through a regular metal detector instead of a body scanner at participating U.S. airports. You'll frequently also encounter shorter security lines. (For frequent international travelers, there's a similar program called Global Entry that costs $100 for five years.)

The other option is to "opt out" of the body scanner. Instead, you'll get a regular

pat-down, at the very least, from a TSA agent. But bear in mind that having to perform pat-downs can make TSA agents very cranky, and if they're in a bad mood, you might be taken into a side room for an even more thorough examination.

Travel with disposable devices — and disposable accounts

You'll likely want to bring some electronic devices with you, such as a smartphone and maybe a laptop, especially if you're traveling on business. But you shouldn't bring your regular smartphone and laptop, especially if you're traveling internationally.

Many customs officials and border guards, including American ones, have the right to examine your electronic devices and your online accounts. They can ask you for the passwords to your phone, your computer, and even your Google, Facebook and Dropbox accounts.

You don't have to give U.S. customs officials your passwords, but if you don't, they can confiscate your devices. Border officials in other countries may be even less friendly.

So instead of traveling with a $1,200 MacBook, travel with a $200 Chromebook. Perform a "power wash" to clear your account and shut down the Chromebook before you cross any border.

And if you have stuff in your online accounts that you'd rather not have border officials see, then set up "fake" Google, Facebook and Dropbox accounts, using your real name, before you travel. Put some stuff in each account — not much, but enough to look real — in each one, and then show border officials those accounts if they ask.

Once you're across the border, log out of the fake Google account and then log back in with your regular Google account. As long as you have internet access, all your data will be restored.

The same strategy goes for smartphones. Leave the iPhone behind, and get a cheap Android phone instead. If you're truly worried about officials seeing your data, then set it up with your fake Google account, and log in to your fake Facebook account before you cross a border. If any nosy official wants to see what's on the phone, gladly provide it.

Use a VPN the whole time

The biggest threat to privacy while traveling, however, comes from unsecured Wi-Fi networks in airports, hotels and restaurants. If any data you transmit from your laptop or phone is unencrypted, anyone else on the same network may be able to read it, even if the network has a password.

Take the baby step up of installing the Electronic Frontier Foundation's HTTPS Everywhere browser plugin on your laptop browsers. The plugin will activate encrypted connections to any website that supports them, including Facebook and Google.

But not all websites support encrypted connections. That's where a VPN (virtual private network) service comes in. The VPN will encrypt all internet traffic between your laptop or smartphone, making sure that all your Wi-Fi data will be unreadable to snoopers on the same network.

If you're traveling on business, ask your company's IT department if there's a company VPN service you can use. We've tested all of the top services; if you're willing to pay for a VPN, check out our picks for the best VPNs.

The Canadian VPN service Windscribe lets you encrypt up to 10GB of data per month for free. The U.S. VPN service Hotspot Shield gives you an unlimited amount for free, but only on mobile devices, and it may also inject ads into the web pages you're viewing.

Smart hotel rooms may be too smart

Hotel rooms may soon collect and use your personal data to customize your experience. Both Marriott and Hilton are working to bring the smart-home concept to their properties.

Marriott's IoT Guestroom Lab, which is currently in testing at the company's headquarters, would let users interact with a virtual assistant to set alarms,

request services and operate various features, including turning on the shower to a specific temperature based on stored preferences.

Hilton's Connected Room is in the pilot phase in one hotel. The goal is for guests to use both voice commands and the Hilton Honors app — which already has check-in and digital-key capabilities— to control temperature, lights and streaming media, and to save custom preferences in their profiles.

While guests may want, or even expect, their hotel rooms to operate like their smart homes, according to a recent University of Delaware study, smart technology isn't risk-free.

For example, Marriott's smart room is designed to go into sleep mode when guests aren't present. This makes the hotel more energy-efficient, but it may also compromise your personal safety and security if it becomes obvious that you are not in your room, EPIC's Scott said.

He also noted that if guests give up seemingly harmless personal data to a hotel, they make it easier both for malicious actors to link that data to more sensitive information, and for law enforcement to access the information without explicit consent.

Before you stay in a smart hotel room, ask to see the hotel company's privacy policy to find out what kind of personal data will be collected, where and how it is stored, who has access to it, whether it is shared with any other entity, and how you can opt in or out of data collection.

"It goes beyond what is necessary to perform a service," Scott added. "There should be clear options for guests, and the option should be to opt in if they so choose — not one where you have to actively opt out."

Rental cars may keep track of where you go

Airports and hotels may be the most obvious places in which traveler data might be collected and potentially compromised, but they aren't the only ones. If you rent a car, the vehicle likely has an event data recorder (EDR). Like an airplane's black box, the EDR collects information about the vehicle's systems, its location and operator behavior as you drive.

While EDR data is most often used to piece together crash reports, and a 2015 federal law states that collected EDR data belongs to a car's owner or leaseholder, it's unlikely that rental-car drivers would be entitled to privacy with regard to EDR data.

If you use a rented or built-in GPS navigation system while driving a rental car, or you connect your phone to your rental car's Bluetooth system, you could be tracked by the car-rental company or hacked by a third party.

Try to delete any navigation history or personal profile you set up in a rented GPS device or in the in-vehicle computer before you return the rental car. Unfortunately, you won't be able to do anything about the EDR data, and if the rental company was actively tracking your movements, then it already has the location data.

Bringing it all back home

This kind of surveillance isn't limited to travelers. Scott said many retailers increasingly use security cameras with facial-recognition capabilities to identify known shoplifters in their brick-and-mortar stores, although only Lowe's would confirm this. License-plate readers used by police are not uncommon in bigger cities.

All this means that your movements can be easily tracked, and that your information can be accessed by law enforcement or may be at risk of being compromised in a data breach. Unfortunately, stores are within their rights to surveil their customers, and you're not allowed to cover up the license plate on a moving vehicle.

One way to avoid this, whether you're traveling or not, is to turn off the Wi-Fi, GPS, and Bluetooth functions on your smartphone when you're not using them. Keeping them on just makes it easier for other people to track you and read your data. The same goes for your laptop when you're out of the house or the office; if you're not using it, fully shut it down instead of just letting it go to "sleep."

These heightened privacy risks shouldn't stop you from traveling, or from going about your daily routine when you're at home. ■

Internet Security for Travelers

This article was originally published on travel expert, Rick Steves blog

The joys of widespread Wi-Fi availability come with the responsibility to take some protective precautions.

Take extra care if using a public terminal — if you must log in to any account, use an incognito window, and be absolutely sure you've logged out.

While you shouldn't be freaked out about your computer use on the road, travelers who are too careless with their digital information open themselves up to significant hassle and expense. Aim for a middle ground of cautiousness and protect your personal information by heeding the following tips.

Safety Tips for Traveling with Your Own Device
If you're taking your devices on the road, be aware that gadget theft is an issue in Europe. Not only should you take precautions to protect your devices from thieves, but you should also configure them for maximum security so that if they are stolen, your personal data will stay private.

First, check that you're running the latest version of your device's operating system and security software. Next, consider tightening your security settings. At the very least, make sure your device is password- or passcode-protected so thieves can't access your information if it's stolen. If it's already protected, consider decreasing the time it takes for the screen to lock when not in use — while it's annoying to have to keep entering your code, that's not nearly as annoying as identity theft (and you can relax your security settings once you're home). For an extra layer of security, consider setting passwords on apps that access key info (such as email or Facebook).

Traveler Tip:
Password protect every device you are bringing with you so that thieves cannot access your information in case the devices are misplaced or stolen!

Many laptops have a file-sharing option. Though this setting is likely turned off by default, it's a good idea to check that this option is not activated on your computer so that people sharing a Wi-Fi network with you can't access your files. (If you're not sure how, do a search for your operating system's name and "turn off file sharing"). Newer versions of Windows have a "Public network" setting that automatically configures your computer so that it's less susceptible to invasion. (Choose this when you first join the network.)

Once on the road, use only legitimate Wi-Fi hotspots. Ask the hotel or café for the specific name of their network, and make sure you log on to that exact one. Hackers sometimes create bogus hotspots with a similar or vague name (such as "Hotel Europa Free Wi-Fi") that shows up alongside a bunch of authentic networks. It's better if a network uses a password (especially a hard-to-guess one) rather than being open to the world. If you're not actively using a hotspot, turn off Wi-Fi so that your device is not visible to others.

Safety Tips for Using Public Computers

It's perfectly safe to use a public computer for tasks that don't require you to log in to an account. For instance, checking train schedules, maps, or museum hours doesn't pose a security risk. The danger lies in accessing personal accounts that require you to enter a login and password (such as email, Facebook, or any ecommerce site).

If you're traveling with your own device, try to make that your sole means of accessing your accounts. But if you'll be relying on hotel-lobby computers or

internet cafés, keep in mind that you have no idea who used that computer last — or who will hop on next. Public computers may be loaded with damaging malware, such as key-logger programs that keep track of what you're typing — including passwords.

If you do need to access personal accounts on a public computer, make sure that the Web browser you use doesn't store your login information. If you have the option of opening an "incognito" or "private" browser window, use it. When you sign in to any site, look for ways to ensure that the browser forgets your user name and password after you log out: For instance, you should click the box for "public or shared computer" or unclick any box that says "stay signed in" or "remember me." It's also a good idea to clear the internet browser's cache, history, and cookies after you're done, so fewer artifacts of your surfing session remain — especially if you've accessed sensitive information (under the browser's "Options" or "Preferences" settings, look for a "Privacy" or "Security" category).

Finally, consider setting up two-step verification for your most important accounts. This requires you to enter not just a password but a second code whenever you log in using an unfamiliar computer (available with many Web-based email and social-networking sites).

Accessing Personal Information Online

While you're away, you may be tempted to check your online banking or credit-card statements, or to take care of other personal-finance chores. Internet security experts advise against accessing these sites entirely while traveling.

Definitely refrain from logging in to personal financial sites on a public computer. Even if you're using your own mobile device at a password-protected hotspot, any hacker who's logged on to the same network may be able to see what you're up to (chances are remote — but it's possible). If you need to access banking information, it's best to do so on a hard-wired connection (i.e., using an Ethernet cable in your hotel room). Otherwise, try to log in via a cellular network, which is safer than any Wi-Fi connection.

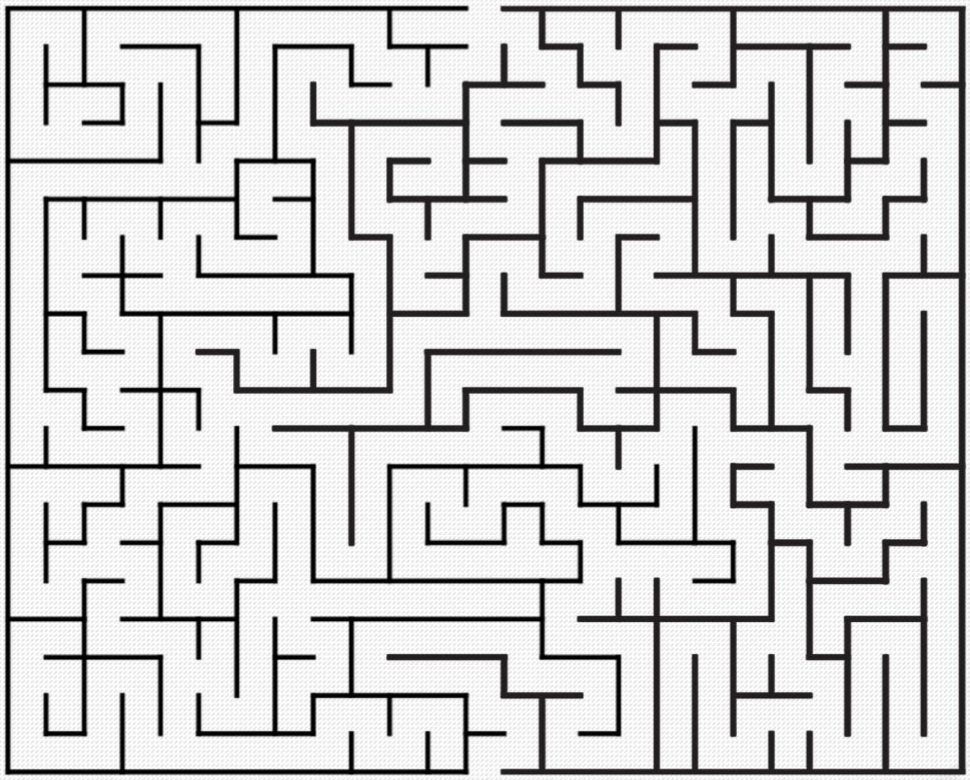
Even if you avoid accessing bank accounts during your trip, you may still need to enter your credit-card information online, such as for booking museum or theater tickets. If so, make sure that the site is secure. Most browsers display a little padlock icon to indicate this; also check that the page's URL begins with https instead of http. Never send a credit-card number (or any other sensitive information) over a website that doesn't begin with https.

For other accounts, such as email, consider upping your security settings while you're on your trip (for example, see Facebook's "extra security features" page). Savvy password habits are also critical. Above all, don't use individual dictionary words, don't reuse passwords (or even similar passwords) across different sites (a password-manager program really helps), and think in terms of using a "passphrase" — the longer your password, the better.

It's also important to be careful if emailing personal information. Don't send your credit-card number in one email message. It's better to call or fax. Some people send their credit-card number in two halves, via two separate email messages. For extra security, a few banks, such as Citi and Bank of America, allow their customers to create virtual account numbers, which are one-time or short-term numbers linked to their regular credit card. ■

HELP THE PRIVACY OFFICER SAFELY
ARRIVE AT HER VACATION DESTINATION

START

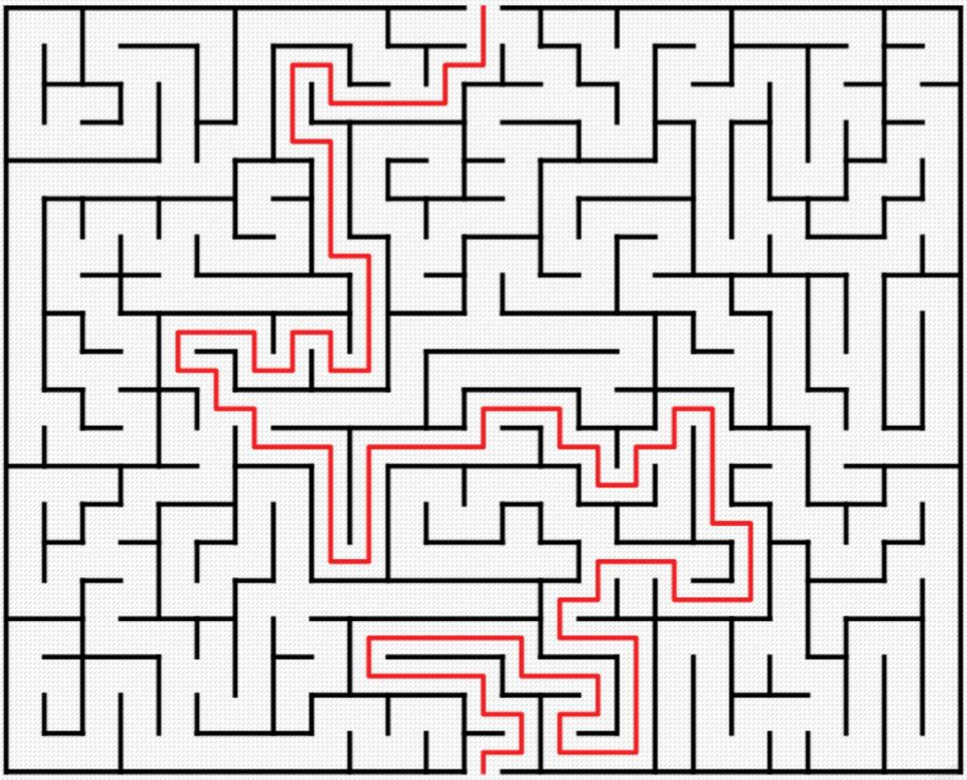


FINISH

Aloha!

HELP THE PRIVACY OFFICER SAFELY
ARRIVE AT HER VACATION DESTINATION

START



FINISH

Aloha!